

Délibération n° 2023-035 du 15 mars 2023

de la Commission de Contrôle des Informations Nominatives portant autorisation à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité

« *Gestion et contrôle des accès physiques aux différents locaux de la banque en Principauté par badges* »

présenté par Bank Julius Baer (Monaco) S.A.M.

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales du Conseil de l'Europe du 4 novembre 1950 ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son Protocole additionnel ;

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu la délibération n° 2010-43 du 15 novembre 2010 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les dispositifs de contrôle d'accès sur le lieu de travail mis en œuvre par les personnes physiques ou morales de droit privé ;

Vu la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la demande d'autorisation déposée par Bank Julius Baer (Monaco) S.A.M. le 7 décembre 2022 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *gestion et contrôle des accès physiques aux différents zones de la banque* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 6 février 2023, conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993 ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 15 mars 2023 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Bank Julius Baer (Monaco) S.A.M. est une société monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 96S03173, ayant entre autres pour objet « *en Principauté de Monaco et à l'étranger, pour son compte ou le compte de tiers, directement ou en participation : La réalisation de toutes opérations de banque ou connexes telles que définies par la "loi bancaire" applicable* ».

Afin d'administrer et de sécuriser l'accès aux locaux de ses deux sites en Principauté, sis Boulevard des Moulins et Avenue de Grande-Bretagne, cette société souhaite procéder à l'installation d'un système de contrôle par badge au sein de son établissement.

Le traitement objet de la présente demande est mis en œuvre à des fins de surveillance, il relève donc du régime de l'autorisation préalable visé à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

Le responsable de traitement indique que ce traitement a pour finalité « *Gestion et contrôle des accès physiques aux différentes zones de la banque* ».

Les personnes concernées sont les salariés, les prestataires longue durée et les intervenants externes.

Enfin, les fonctionnalités sont les suivantes :

- assurer la sécurité des biens et des personnes par la ségrégation des accès entre les clients, le personnel et les intervenants extérieurs ;
- assurer la sécurité des personnes et des biens en contrôlant les accès aux locaux identifiés comme sensibles bénéficiant d'une circulation limitée ;
- gérer les habilitations d'accès aux personnes autorisées ;
- désactiver les badges perdus/volés ;
- permettre la constitution de preuves.

La Commission rappelle toutefois que tout traitement d'informations nominatives doit avoir une finalité « *déterminée, explicite et légitime* » aux termes de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

En l'espèce, la finalité du présent traitement doit être plus explicite c'est-à-dire être claire et précise pour les personnes concernées en précisant que ce contrôle des accès concerne les différents locaux de la banque en Principauté et s'effectue au moyen d'un badge.

Par conséquent, elle modifie la finalité comme suit : « *Gestion et contrôle des accès physiques aux différents locaux de la banque en Principauté par badges* ».

II. Sur la licéité et la justification du traitement

Le traitement est justifié par la réalisation d'un intérêt légitime poursuivi par le responsable de traitement, sans que ne soient méconnus ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

A cet égard, la Commission constate que « *Ce traitement permet à la banque Julius Baer d'assurer la protection des personnes et des biens ainsi que d'assurer la confidentialité des données détenues grâce à une restriction d'accès aux locaux aux seules personnes dûment habilitées* ».

Le responsable de traitement précise par ailleurs qu'il « *permet également de découper les locaux par Zones d'habilitation permettant une ségrégation des accès aux zones sensibles* ».

Enfin, la Commission prend acte que ledit traitement « *n'a pas pour objet de contrôler de manière inopportune les comportements, les habitudes et les horaires des personnes concernées* ».

Elle considère donc que le traitement est licite et justifié conformément aux dispositions des articles 10-1 et 10-2 de la Loi n°1.165 du 23 décembre 1993.

III. Sur les informations traitées

Les informations nominatives traitées sont :

➤ Pour les salariés et prestataires longue durée :

- identité : nom, prénom, photo (obligatoire pour les salariés mais facultative pour les prestataires) ;
- vie professionnelle : société, service, responsable hiérarchique, plage horaire autorisée, zone d'accès autorisée ;
- données liées au badge : numéro, code pin (uniquement pour certaines catégories de salariés ou prestataires) ;
- informations temporelles : date et heure de passage à une zone, nom et/ou numéro du point de passage ;
- logs : logs de connexion des personnes habilités à avoir accès au traitement.

Les informations relatives à l'identité, à la vie professionnelle et aux badges ont pour origine les personnes concernées ou le traitement ayant pour finalité « *Gestion administrative des salariés* ».

Les informations temporelles ont pour origine le dispositif de contrôle.

Enfin, les logs ont pour origine les serveurs de la banque.

➤ Pour les intervenants externes (badge « *visiteur* »)

- identité : nom, prénom ;
- vie professionnelle : société ;
- données liées au badge : numéro ;
- données liées aux badges : date et heure de remise et de récupération du badge ;
- informations temporelles : date et heure de passage à une zone, nom et/ou numéro du point de passage.

Ces informations ont pour origine les personnes concernées et sont conservées sur support papier.

Les informations temporelles ont pour origine le dispositif de contrôle.

La Commission considère donc que les informations collectées sont « *adéquates, pertinentes et non excessives* » au regard de la finalité du traitement, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

IV. Sur les droits des personnes concernées

➤ *Sur l'information préalable des personnes concernées*

L'information préalable des personnes concernées est effectuée par le biais d'une mention ou clause particulière intégrée dans un document remis à l'intéressé ainsi que par une procédure interne accessible en Intranet.

A cet égard, la Commission rappelle que ceux-ci doivent impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Elle rappelle par ailleurs que cette information préalable doit être effectuée auprès de toutes les personnes concernées par le traitement dont s'agit, et notamment de l'ensemble intervenants externes.

En conséquence, la Commission demande que soit assurée l'information préalable de ces derniers, conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

➤ *Sur l'exercice du droit d'accès, de modification et de mise à jour*

Le droit d'accès s'exerce par voie postale, par courrier électronique ou sur place auprès du Directeur Juridique et Data Protection Officer.

A cet égard, la Commission rappelle que la réponse à un droit d'accès doit intervenir dans le mois suivant la réception de la demande.

Elle considère par ailleurs qu'une procédure devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations. A ce titre, elle précise que si une copie d'un document d'identité était demandée, la transmission et le traitement de ce document devront faire l'objet de mesures de protection particulières comme rappelé dans sa délibération n° 2015-113 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Sous cette condition, la Commission constate que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 de la Loi n° 1.165 du 23 décembre 1993.

V. Sur les personnes ayant accès au traitement et les destinataires

➤ *Sur les destinataires*

Les informations sont susceptibles d'être communiquées aux Autorités policières ou judiciaires.

La Commission estime à cet effet que la communication à la Direction de la Sûreté Publique peut être justifiée pour les besoins d'une enquête judiciaire.

A cet égard, elle rappelle qu'en cas de transmission, ladite Direction ne pourra avoir communication des informations que dans le strict cadre de ses missions légalement conférées.

La Commission considère donc que ces transmissions sont conformes aux exigences légales.

➤ **Sur les personnes ayant accès au traitement**

Les personnes habilitées à avoir accès au traitement sont :

- les membres des Services Généraux (Monaco): initialisation de la demande, consultation, demande de modification ;
- la Directrice Opérationnelle (Monaco) : demande de modification ;
- les membres de l'équipe Global Pers ; & Phys Security (Suisse) : tous droits à la demande des Services Généraux ou de la Directrice Opérationnelle ;
- le prestataire en charge du matériel : maintenance (aucun accès aux données).

Considérant les attributions de chacune de ces personnes, et eu égard à la finalité du traitement, les accès susvisés sont justifiés.

En ce qui concerne le prestataire, la Commission rappelle que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les droits d'accès doivent être limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestation de service. De plus, ledit prestataire est soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

Elle rappelle enfin qu'en application de l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993 la liste nominative des personnes ayant accès au traitement doit être tenue à jour, et précise que cette liste doit lui être communiquée à première réquisition.

VI. Sur les rapprochements et interconnexions avec d'autres traitements

Le responsable de traitement indique que le présent traitement fait l'objet d'une interconnexion avec un traitement ayant pour finalité « *Gestion administrative des salariés* ».

La Commission prend acte que ce traitement a été légalement mis en œuvre.

VII. Sur la sécurité du traitement et des informations

Les mesures prises pour assurer la sécurité et la confidentialité du traitement et des informations qu'il contient n'appellent pas d'observation particulière.

La Commission rappelle néanmoins que les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

Elle constate que la copie ou l'extraction d'informations issues de ce traitement est chiffrée sur son support de réception.

La Commission rappelle également que, conformément à l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par celui-ci et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état

de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du présent traitement.

VIII. Sur la durée de conservation

Les informations relatives à l'identité et à la vie professionnelle ainsi que les données liées au badge sont conservées 3 mois à compter du départ de la société pour les salariés et les prestataires et 3 mois à compter de la date de la fin de la visite pour les visiteurs.

Concernant les photos des salariés et prestataires longue durée, la Commission prend acte que celles-ci figurent uniquement sur les badges et ne sont pas conservées dans le système.

Les logs sont conservés 1 an.

Enfin, les informations temporelles sont conservées 1 an.

A cet égard, la Commission rappelle, conformément à sa délibération n° 2010-43 du 15 novembre 2010, que ces informations ne peuvent être conservées sous une forme permettant l'identification de la personne concernée que pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour lesquelles elles ont été collectées.

Aussi, elle fixe la durée de conservation des informations temporelles à 3 mois.

Après en avoir délibéré, la Commission :

Modifie la finalité du traitement par « *Gestion et contrôle des accès physiques aux différents locaux de la banque en Principauté par badges* ».

Constata que la copie ou l'extraction d'informations issues de ce traitement est chiffrée sur son support de réception.

Considère qu'une procédure relative au droit d'accès par voie électronique devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations.

Rappelle que :

- les documents d'information doivent impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;
- la réponse au droit d'accès doit intervenir dans le mois suivant la réception de la demande ;
- la Direction de la Sûreté Publique ne pourra avoir communication des informations que dans le strict cadre de ses missions légalement conférées ;
- la liste nominative des personnes ayant accès au traitement doit être tenue à jour et doit lui être communiquée à première réquisition ;
- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

Demande que soit assurée l'information préalable de l'ensemble des intervenants externes, conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Fixe la durée de conservation des informations temporelles des salariés et des prestataires à 3 mois.

A la condition de la prise en compte de ce qui précède,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par Bank Julius Baer (Monaco) S.A.M. du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et contrôle des accès physiques aux différents locaux de la banque en Principauté par badges* ».**

Le Président

Guy MAGNAN